Transposition of the Fifth Money Laundering Directive – HMT consultation dated April 2019

Response from TISA

Date 10 June 2019

About TISA

TISA is a unique, consumer focused membership organisation. Our aim is to improve the financial wellbeing of UK consumers by aligning the interests of people, the financial services industry and the UK economy. We achieve this by delivering innovative, evidence-based proposals to government, policy makers and regulators; the proposals provide practical solutions to major consumer issues.

TISA's growing membership comprises over 190 firms involved in the supply and distribution of savings and investment products and services. These members represent all sectors of the financial services industry, including the UK's major investment managers, retail banks, insurance companies, pension providers, distributors, building societies, wealth managers, third party administrators, FinTech, consultants and advisers, software providers, financial advisers, pension providers, banks and stockbrokers.

TISA's current strategic policy and industry solution developments include:

- **Guidance**: developing a framework to make guidance more widely available to the estimated 42 million UK citizens who will rely on it when making financial decisions;
- **Digital ID:** development of a digital identity for consumers of financial services: following successful earlier feasibility work, a project with members has now been established to develop and test a pilot of the Digital ID;
- **Digitalisation**: building on the successful launch of TeX, TISA has initiated a range of member projects developing open standards that support the growth of FinTech and increase consumer access to financial services, while lowering costs for providers;
- **Financial education**: helping to make young people aware of the impact of finance on their life including the KickStart Money project – a £1million three-year programme delivering financial education to 18,000 primary school children;
- **Retirement saving**: strategic policy focused on the needs of millennials and the self-employed and the use of property to supplement retirement income;
- **ISAs**: working with government, the simplification/improvement of this key savings regime;
- **The TISA and KPMG Savings Index:** a biannual measure of typical household savings and debt in Great Britain;
- **Consumer engagement:** alongside our financial education and guidance work, we are also considering how the industry can improve how they identify and interact with vulnerable customers, and encourage greater financial capability for UK consumers.

TISA also provides support on a range of operational and technical issues targeted at improving processes, standards of good practice and open standards, alongside the interpretation and implementation of new rules and regulations, including MiFID II (through publication of good practice guides and open standards, and an industry solution to the collection of target market data and costs & charges); Client Assets (publishing good practice guides and working on unbreakable term deposits; tackling financial crime, data standards, SM&CR and GDPR; and Brexit, by developing proposals for

government that will enable the savings and investments sector to prosper on a global scale to the benefit of UK plc.

Our work to improve industry infrastructure includes TeX, (an industry utility providing the legal framework and governance necessary for the use of electronic messages facilitating transfers) alongside support for the Transfers & Re-registration Industry Group (TRIG) and support for the UK Fund Trading and Settlement initiative (FTS).

……

Our response to some of the question are shown below. Where we have not listed a question it is because we have no comment.

Cryptoassets

Q12: 5MLD defines virtual currencies as "a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically". The Government considers that all relevant activity involving exchange, security and utility tokens should be captured for the purposes of AML/CTF regulation, and seeks views on this approach. Is the 5MLD definition appropriate or does it need to be amended in order to capture these three types of cryptoassets (as set out in the Cryptoassets Taskforce's framework)? Further, are there assets likely to be considered a virtual currency or cryptoasset which falls within the 5MLD definition, but not within the Taskforce's framework?

> In view of the rapidly evolving nature of virtual currencies and their like, and the ingenuity of the online community (referring here to both legitimate and illegitimate operators) we recommend that the transposition of 5MLD allows for as broad and as flexible a definition of virtual currency as is legally viable.

Q13: 5MLD defines a custodian wallet provider as "an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies". The Government considers that all relevant activity involving exchange, security and utility tokens should be captured for the purposes of AML/CTF regulation, and seeks views on this approach. Is the EU Directive definition appropriate or does it need to be amended in order to capture these three types of cryptoassets (as set out in the Cryptoassets Taskforce's framework)? Further, are there wallet services or service providers likely to be considered as such which fall outside this Directive definition, but should come within the UK's regime?

> The 5MLD definition seems sufficiently comprehensive but our response to Q12 above is also relevant here.

Q14: Should the FCA be assigned the role of supervisor of cryptoasset exchanges and custodian wallet providers? If not, then which organisation should be assigned this role?

> The FCA is the obvious choice from existing candidates, particularly given its existing role as Payment Systems Regulator. However, we would like HMT to consider the

potential for a new AML regulator with oversight of economic crime risks across all industry sectors, not just financial services. We expand on this in answer to questions 44, 45 and 46.

Q15: The government would welcome views on the scale and extent of illicit activity risks around cryptoassets. Are there any additional sources of risks, or types of illicit activity, that this consultation has not identified?

The Consultation is realistic in recognising the attraction to the criminal fraternity of cyptoassets and the rapidly developing risks they present. We can be sure that any list of risks and illicit activities identified today will not be comprehensive tomorrow.

Q16: The government would welcome views on whether cryptoasset ATMs should be required to fulfil AML/CTF obligations on their customers, as set out in the regulations. If so, at what point should they be required to do this? For example, before an 'occasional transaction' is carried out? Should there be a value threshold for conducting CDD checks? If so, what should this threshold be?

Generally we see no reason why cryptoasset transactions should not be subject to the same AML standards as applies to fiat currency transactions.

Q17: The government would welcome views on whether firms offering exchange services between cryptoassets (including value transactions, such as Bitcointo-Bitcoin exchange), in addition to those offering exchange services between cryptoassets and fiat currencies, should be required to fulfil AML/CTF obligations on their customers.

We agree. See our response to Q16.

Q18: The government would welcome views on whether firms facilitating peer to-peer exchange services should be required to fulfil AML/CTF obligations on their users, as set out in the regulations. If so, which kinds of peer-to peer exchange services should be required to do so?

We agree. See our response to Q16.

Q19: [No comment.]

Q20: The government would welcome views on whether firms involved in the issuance of new cryptoassets through Initial Coin Offerings or other distribution mechanisms should be required to fulfil AML/CTF obligations on their customers (i.e. token purchasers), as set out in the regulations.

We agree. See our response to Q16.

Q21 to Q23: [No comment.].

Q24: The global, borderless nature of cryptoassets (and the associated services outlined above) raise various cross-border concerns regarding their illicit abuse, including around regulatory arbitrage itself. How concerned should the government be about these risks, and how could the government effectively address these risks?

The government should indeed be concerned. It is perhaps a political and therefore not immediately useful point but the borderless and global nature of the still emerging cryptoasset ecosystem threatens the concept of the nation state as a democratic and governable unit. There is a significant population amongst advocates of cryptoassets who cynically, and even openly, see the evolution of cryptoassets as a direct challenge to any government and an escape from geographically grounded legal systems. There are many who see cryptoassets as an escape from systems of taxation, sanctions, press intrusion and political interference. It is therefore vital that governments across the developed world co-operate to develop coherent, homogenous and co-ordinated legal systems to meet these threats. In this regard Brexit can be regarded as a potential risk, although of course much depends in what form, if at all, Brexit takes.

Q25: What approach, if any, should the government take to addressing the risks posed by "privacy coins"? What is the scale and extent of the risks posed by privacy coins? Are they a high-risk factor in all cases? How should CDD obligations apply when a privacy coin is involved?

We have no data on the usage of privacy coins, and obviously the risk level posed by them depends on their prevalence. From a layman's perspective any token that is deliberately designed to hide the identity of the holder must be a concern from an AML viewpoint.

Customer due diligence

We would like to provide a combined answer to questions 44, 45 and 46:

Q44: Is there a need for additional clarification in the regulations as to what constitutes "secure" electronic identification processes, or can additional details be set out in guidance?

Q45: Do you agree that standards on an electronic identification process set out in Treasury-approved guidance would constitute implicit recognition, approval or acceptance by a national competent authority?

Q46: Is this change likely to encourage firms to make more use of electronic means of identification? If so, is this likely to lead to savings for financial institutions when compared to traditional customer onboarding? Are there any additional measures government could introduce to further encourage the use of electronic means of identification?

Background

We believe TISA is in a strong position to respond to these questions for two reasons:

- TISA is working with our members to develop an electronic identification scheme for the Financial Services sector, which will be compliant with the AML regulations. (The scheme may be rolled out to other sectors.) This project is being led by TISA's Digital Innovation Director Harry Weber-Brown, who has been providing regular updates to the FCA, the Treasury and is

working closely with other parts of the Government (such as the Gov.UK Verify team in GDS).

- The Consultation refers to the potential role of JMLSG. TISA is a member firm of the JMLSG. On 14 March 2019 Mr Weber-Brown gave the JMLSG Board an overview of TISA's project and its progress to date, which prompted a useful discussion. Although we understand that the JMLSG Board intends to respond to the Consultation on its own account we provide below our own understanding of the role of JMLSG, which we believe inhibits its ability to meet the Consultation's suggestions.

It is vital in our view that any discussion in relation to the 5MLD's proposals regarding electronic identification is undertaken with an understanding of the substantial benefits that could accrue to the UK, if the opportunity is grasped to implement a nationwide electronic identification programme that is made available to private sector. The 5MLD document is aimed at improving resistance to crime and it recognises and encourages EU member states to consider implementing them but for obvious reasons it does not highlight the commercial and societal benefits that such schemes can bring:

A successful, nationwide, electronic identification scheme (or schemes) will bring significant benefits in terms of reducing the regulatory burden on firms, through shared identity data, and it provides a better customer experiences by removing the need to repetitively submit identity data to online services. It can also assist vulnerable consumers to gain access to financial services. There is an opportunity here that has been recognised in other EU states but so far seems to have been overlooked in the UK, to the detriment of UK plc.

To replay the Consultation's comments in response to 5MLD's proposals: *Nothing in the existing UK regulations precludes the use of electronic means of identification, but the addition of this explicit mention of electronic identification may provide greater* ***clarity for firms****. The requirement for electronic identification processes to be "regulated, recognised, approved or accepted at national level by the national competent authority" in order to be taken into account does not require formal recognition by regulators for a particular identification scheme – approval from the competent national authority can be implicit. The government welcomes views on whether* ***standards on an electronic identification process*** *set out in Treasury-approved guidance (such as that published by the Joint Money Laundering Steering Group) would constitute implicit recognition."*

TISA would like seek clarification in relation to a) the Directive's intention, b) the regulatory position, c) challenges relating to scheme recognition and the responsibilities of an MLRO, and d) JMLSG's remit and responsibilities. To take each of these issues in turn:

The Directive's intention and interpretation

We question the assumption that compliance with 5MLD *'does not require formal recognition by regulators'.* That seems to us to be precisely what 5MLD does demand; the words "*secure remote or electronic identification processes, regulated, recognised, approved or accepted at national level by the national competent authority"* do not seem to us to allow for any alternative interpretation.

We accept the obvious difficulty; that there is not currently any obvious candidate for the role of national competent authority, and we comment on this below in our suggestions regarding the possible way forward under the heading 'Conclusions'.

The regulatory position; the 'Reliance' challenge

The Consultation's response paragraph starts with the statement: *"Nothing in the existing UK regulations precludes the use of electronic means of identification".* Whilst this is true to an extent - firms are permitted to recognise electronic documents - it is not true in relation to Digital ID or 'Digital passport' schemes of the kind that is discussed in the Directive. This statement does not appear to take into account the 'Reliance' rules as laid down in the UK's Money Laundering Regulation 17 which prohibits firms from relying on due diligence (i.e. 'Know Your Customer' checks) performed by another party save for a few special situations:

In basic terms a regulated[1] firm (Firm 'A') is permitted to rely on another firm's (Firm 'B') due diligence provided that **either**: Firm B has a contractual relationship with Firm A such that it (Firm B) is effectively providing outsourced services to Firm A, **or**; Firm B is acting as Firm A's agent in a contractual relationship in which Firm A is the principal in the relationship, **and** Firm B is authorised and regulated under the ML rules in its own right (as it would need to be to act as an firm involved in ML-regulated activities). In either scenario above Firm B must consent to Firm A placing reliance upon its (Firm B's) due diligence activities. In either scenario both firms must accept that Firm A remains responsible for the due diligence standards achieved by Firm B, and liable for any failure on Firm B's part to conduct adequate due diligence. To meet this responsibility Firm A must define the standards required, and have adequate measures in place to monitor Firm B's performance. Firm B must also be ready to provide whatever assurance and evidence Form A might reasonably demand in that regard, for five years after the termination of the relationship between the two firms.

So the statement that "*"Nothing in the existing UK regulations precludes the use of electronic means of identification"* does not appear to be wholly true. The ML regulations explicitly prevent a firm from accepting electronic identification, where that identification has been verified by a firm with whom it does not have a direct contractual relationship. This may be the case where a Digital ID scheme has a central Governance Body with whom a participating firm has a contractual relationship, rather than all participant firms being required to have (multi-lateral) contracts with each of the participating firms. This in turn means that any ID provided by an independent electronic ID provider cannot be accepted by a third party firm, which would render that ID of little use or value to a consumer. This is a major obstruction to any implementation of an electronic identification scheme in the UK. This is an issue that should be addressed in the implementation of 5AMLD.

The Recognition (MLRO) challenge

We also do not agree with the Consultation's next statement: *"The requirement for electronic identification processes … does not require formal recognition by*

[1] i.e. a firm caught by the money laundering regulations. This need not be a financial services firm; the EU legislation refers to 'obliged entities' in this regard, and the ML Regs refer to 'relevant persons'. We use the word 'regulated' here in its generic sense.

regulators for a particular identification scheme - approval from the competent national authority can be implicit."

We do not see that any recognition by a competent national authority might practicably be given on an '*implicit'* basis. Competent authorities (such as regulators) will not normally provide informal or implicit recognition; their role is to provide formal, explicit guidance and, where appropriate, recognition. In this regard the Consultation's proposal fails to take into account the Money Laundering Reporting Officer's ('MLRO') challenge. MLROs carry personal responsibility and legal liability for ensuring that their firm demonstrably meets its obligations to conduct adequate customer due diligence. Asking an MLRO to take accept a customer's *bona fides* based on independently verified third party electronic identity created under a scheme which has only "*implicit"* recognition by a competent authority would be unlikely to satisfy any sensible and diligent MLRO, who must be able to justify his or her decision to accept a customer's ID.

The JMLSG challenge

The Consultation document goes on to say: "*The government welcomes views on whether standards on an electronic identification process set out in Treasury-approved guidance (such as that published by the Joint Money Laundering Steering Group) would constitute implicit recognition."*

The JMLSG's responsibility is to interpret existing laws and regulations, producing helpful guidance for industry practitioners on how those laws and regulations might be met. Although its guidance is approved by HMT it is not statutory; it is up to an individual MLRO to apply whatever standards he or she sees as appropriate in meeting the legal and regulatory obligations. The JMLSG does not, and cannot, recognise, approve or accept any other party's methods or approach to meeting the obligations, nor is it a competent authority allowing it to act as any kind of regulator. It is certainly not in the business of making any 'implicit' statements; its aim is to clarify and make explicit the laws and rules of the UK.

Conclusion

We accept that 5MLD is principally aimed at improving member states' resistance to financial crime. However the Consultation seems to overlook the significant opportunities available to the UK, in responding to 5MLD, for providing certainty and trust to financial services in the use of Digital Identity schemes. The benefits that would accrue from this include:

- Better access for customers to services of all kinds, not just financial services;
- Better access and protection for customers who are not necessarily IT 'savvy', or who are vulnerable;
- Improved competitiveness for UK-based businesses as they extend their offerings to overseas buyers and business partners.

We suggest below the steps HMT might wish to consider in order to take advantage of these opportunities:

1. The establishment of a national competent authority with responsibility for economic crime, across all industries (not just FS), funded by those industries.

This seems to us to be linked to the government's own recent proposals for the establishment of a new Economic Crime Strategic Board (ECSB); a single cross-government Ministerial Board to drive the public and private sector response to economic crime with a view to developing a public-private economic crime plan.

2. Urgent consideration given by the ECSB (or any body it cares to establish) to review the ML regulation's 'Reliance' requirements in the context of electronic identification schemes. In this regard we note HMT's own proposals to *"lead a comprehensive review of the effectiveness and scope of the Money Laundering Regulations 2017 (MLRs) and publish a report before 26th June 2022".* It seems to us vital that this review takes into account the considerable benefits that would accrue from recognising privately funded electronic identification schemes, untrammelled by the ML regulations' Reliance obstacles.

3. Publication by HMT, or by any body it cares to nominate, of guidance in relation to the standards required of privately funded electronic identification schemes seeking recognition / approval by the nominated national competent authority.

Q47: To what extend would removing 'reasonable measures' from regulation 28(3)(b) and (4)(c) be a substantial change? If so, would it create any risks or have significant unintended consequences?

Our view is that many firms already apply the CDD standards described here, so we are generally supportive of the proposal.

Q48: Do you have any views on extending CDD requirements to verify the identity of senior managing officials when the customer is a body corporate and the beneficial owner cannot be identified? What would be the impact of this additional requirement?

Again, we believe that most firms already apply this approach, so we are generally supportive of the proposal as having low impact.

Q49: Do related ML/TF risks justify introducing an explicit CDD requirement for relevant persons to understand the ownership and control structure of customers? To what extent do you already gather this information as part of CDD obligations?

As for our response to Q47 and 48. We agree.

Q50: Do respondents agree we should clarify that the requirements of regulation 31 extend to when the additional CDD measures in regulation 29 and the EDD measures in regulations 33-35 cannot be applied?

We agree.

Q51 & Q52: We have no comment.

Obliged entities: beneficial ownership requirements

Q53: Do respondents agree with the envisaged approach for obliged entities checking registers, as set out in this chapter (for companies) and chapter 9 (for trusts)?

JMLSG guidance permits business relationships to be entered into before DD is undertaken; the obligation to perform DD must precede a relevant transaction. We would be grateful for clarification of this point.

Q54: Do you have any views on the government's interpretation of the scope of 'legal duty'?

This accords with current practice in most firms to review on a risk-rated basis all ongoing client (or other relevant business) relationships on an annual or other appropriate timetable.

Q55: Do you have any comments regarding the envisaged approach on requiring ongoing CDD?

No.

Enhanced due diligence

Q56: Are there any key issues that the government should consider when defining what constitutes a business relationship or transaction involving a high-risk third country?

We are concerned at the wording used here. 'Involving' is a subjective phrase open to interpretation. Up to now the understanding has been to look at risks relating to where an entity is established. 'Involving' could relate to a wide range of factors and we would be grateful for clarification on this point.

Q57: Are there any other views that the government should consider when transposing these Enhanced Due Diligence measures to ensure that they are proportionate and effective in combatting money laundering and terrorist financing?

We disagree with the proposal in Section 6.14. Dual nationality carries its own risks, particularly where the individual is a national of a higher-risk country. Many terrorists for example are often reported to be dual nationals. Having a British passport should not be allowed to act as carte blanche; firms should take into account the second (or any other) nationality.

Q58: Do related ML/TF risks justify introducing 'beneficiary of a life insurance policy' as a relevant risk factor in regulation 33(6)? To what extent is greater clarity on relevant risk factors for applying EDD beneficial?

We do not understand FATF's views on this matter. We would be grateful for clarity on how or why it should be considered a relevant risk factor.

Politically exposed persons: prominent public functions

Q59: Do you agree that the UK functions identified in the FCA's existing guidance on PEPs, and restated above, are the UK functions that should be treated as prominent public functions?

We agree, although we would also like to see stronger measures to ensure that the PEPs themselves are aware of their status and the regulatory implications of this.

Q60: Do you agree with the government's envisaged approach to requesting UK headquartered intergovernmental organisations to issue and keep up to date a list of prominent public functions within their organisation?

We agree.

Mechanisms to report discrepancies in beneficial ownership information

Q61: Do you have any views on the proposal to require obliged entities to directly inform Companies House of any discrepancies between the beneficial ownership information they hold, and information held on the public register at Companies House?

We do not support these proposals. Due diligence often identifies discrepancies and it is the responsibility of the obliged entity to seek satisfactory explanation from the firm of those discrepancies. It is then the duty of the firm to resolve the discrepancies at Companies House; this duty should not fall to the obliged entity. Larger firms are in constant communication with Companies House to inform them of changes to directors, etc, and dual reporting from the obliged entity is likely to simply cause confusion.

Q62: Do you have any views on the proposal to require competent authorities to directly inform Companies House of any discrepancies between the beneficial ownership information they hold, and information held on the public register at Companies House?

For similar reasons to the above we do not support these proposals. The competent authority has a duty, at the time of either a regulated firm's application for authorisation or an individual's application for approval, to conduct due diligence on the applicant, thereby ensuring that the information provided in the application matches that held at Companies House. This duty is a one-off function and should not be ongoing, as discrepancies will constantly arise.

Q63: How should discrepancies in beneficial ownership information be handled and resolved, and would a public warning on the register be appropriate? Could this create tipping off issues?

We are not able to comment on this question.

Trust registration service

Q64 to Q81: We are generally supportive of the Consultation's proposals here, although we would like more clarity on who will have access to the Register.

National register of bank account ownership

Q82 to Q87: Again we are generally supportive of the Consultation's proposals here, although (again) much will depend on who will have access to the Register.